JAMES E. WHITMIRE
Nevada Bar No. 6533
SANTORO WHITMIRE
10100 W. Charleston Blvd., Suite 250
Las Vegas, Nevada 89135
Telephone: (702) 948-8771
Facsimile: (702) 948-8773
jwhitmire@santoronevada.com

JOHN C. CLEARY
(*pro hac vice* forthcoming)
POLSINELLI PC
600 Third Avenue, 42nd Floor
New York, New York 10016
Telephone: (212) 413-2837
Facsimile: (212) 684-0197
john.cleary@polsinelli.com

MARK A. OLTHOFF
(*pro hac vice* forthcoming)
CATHERINE A. GREEN
(*pro hac vice* forthcoming)
POLSINELLI PC
900 W. 48th Place, Suite 900
Kansas City, Missouri 64112-1895
Telephone: (816) 753-1000
Facsimile: (816) 753-1536
molthoff@polsinelli.com
cgreen@polsinelli.com
Attorneys for Defendants

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

JEHU BRYANT, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

MX HOLDINGS US, INC., CFP FIRE PROTECTION, INC., COSCO FIRE PROTECTION, INC. and FIRETROL PROTECTION SYSTEMS, INC.,

Defendants.

Case No. 2:22-cv-00855-GMN-EJY

DEFENDANTS' MOTION TO DISMISS AND MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

Defendants MX Holdings US, Inc., CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc. (collectively, "Defendants") move to dismiss Plaintiff

Jehu Bryant's Class Action Complaint ("Complaint") for lack of subject matter jurisdiction and failure to state a claim upon which relief can be granted.[1]

INTRODUCTION

Plaintiff Jehu Bryant ("Plaintiff") has filed suit against Defendants for alleged injury to himself and a putative class of "thousands" of others from a data security incident involving Defendants' email system (the "Incident"). *See* Compl., ¶ 1. Defendants disclosed the Incident on May 10, 2022 and notified Plaintiff on or about that date via letter. *See id.*, ¶ 26 (citing the notice letter received by Plaintiff (the "Notice Letter")). The Notice Letter, although not attached to the Complaint, is nevertheless part of the Complaint and will govern where, as here, Plaintiff offers contradictions, strained interpretations and wholesale conjecture about the Incident in his efforts to plead a viable case under Nevada law. No such case has been pleaded here, and Plaintiff's Complaint should be dismissed.

FACTS CONCERNING THE INCIDENT

Plaintiff is "a natural person residing in Clark County, Nevada." *See* Compl., ¶ 14 (ECF No. 1.). He claims to have entered into an "employment and services" contract or "employment services" contract with one or more of the Defendants, *see id.*, ¶¶ 75, 81, but does not specify which Defendant and does not provide a copy of the "valid and enforceable express contracts" or other "contracts" between him and such Defendant, as referred to in the Complaint. *See id.*, ¶¶ 64,

[1] This motion addresses Plaintiff's allegations and not those of absent class members. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975) ("Petitioners must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.") (internal quotation marks omitted); *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n. 20 (1976) (same). Defendants further reserve their rights to challenge any putative class, including the elements of Rule 23, the scope of any putative class, and the Court's jurisdiction over non-resident putative class members. *See* Fed. R. Civ. P. 12(b)(2), 23.

65, 67, 68. Indeed, the sole cited basis for Plaintiff's knowledge of Defendants or the Incident is the Notice Letter itself. *See id.*, ¶¶ 26, 79, 83.

The Notice Letter template that was the basis for the letter sent to Plaintiff is attached hereto as **Exhibit A** and is identical in all material respects to such letter. The cover note is as follows:

> On behalf of MX Holdings US, Inc. and its subsidiaries, including CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc., we are writing to inform you of a recent incident that *may have resulted in the temporary exposure of some of your personal information*. We value the trust you place in our organization. *We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft*. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.
>
> **What Happened?** On or about October 28, 2021, we observed suspicious activity within our email system. We immediately engaged a third-party forensic security firm to investigate the issue and confirm the security of our computer systems. This investigation determined that *an unauthorized third party was able to temporarily access several email accounts*. Additionally, we promptly retained a specialized document review vendor to examine the email accounts to determine whether any personal information was contained in the accounts.
>
> **What Information Was Involved?** On or about April 5, 2022, we determined that the relevant email accounts contained certain personal information. *That information varied by individual, but may have included your name, date of birth, Social Security number, driver's license number, passport number, financial account number, and/or limited medical information*.
>
> **What We Are Doing.** In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect yourself.
>
> Finally, although *we are not aware of any instances of fraud or identity theft resulting from this incident, in an abundance of caution, we are offering a complimentary one-year membership of myTrueIdentity online Credit Monitoring by TransUnion*. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. . . .

Exhibit A at 1 (emphasis added); *see also* Compl., ¶ 26 (citing Notice Letter).

Notwithstanding the Notice Letter, Plaintiff inexplicably alleges that his personal information was in fact accessed and stolen in the Incident. *See, e.g.,* Compl., ¶ 1 (alleging personal information "was *stolen* by cybercriminals" in the Incident) and ¶ 6 ("Plaintiffs' and Class Members' sensitive personal information . . . was compromised, unlawfully accessed, and *stolen* due to the Data breach.") (emphasis added).

No such statement of fact appears in the Notice Letter, however. Nor is there any basis on which any such factual averment can be inferred or deemed true from the circumstances. Indeed, the Notice Letter says exactly the opposite – the nature and extent of data compromise in the Incident was limited but indeterminate in certain respects and the Notice Letter and offer of credit monitoring were sent to Plaintiff in an abundance of caution, not because Plaintiff's personal information was in fact compromised or stolen.

In terms of actual adverse impact or injury from the Incident, the Complaint says nothing at all. Although Plaintiff makes a conclusory allegation that he believes he has been "harmed" (Compl., ¶ 7), he does not allege any actual harm. Plaintiff speculates only that he has "been exposed to a substantial and present risk of fraud and identity theft." (Compl. ¶ 35). Plaintiff alleges that he "lost the benefit of his bargain" with Defendants (Compl. ¶ 34), but never comes close to explaining what exactly this "bargain" was and how exactly Defendants have now fallen short of his expectations.[2] Indeed, the plethora of documents and other paraphernalia cited in Count III (Breach of Contract) and Count IV (Breach of Implied Contract) make these claims not only implausible on their face, but almost completely unintelligible to Defendants as a group or

[2] To be sure, there are references in the Complaint to Defendants' alleged violations of their "Notices of Privacy Practices," *see, e.g.*, Compl., ¶¶ 79, 80, 83, but these are obviously boilerplate allegations having nothing to do with Defendants or the industrial sector they occupy ("building construction, safety, and fire protection services"). *Id.*, ¶ 15. These Notices are instead required in the health care sector. *See* 45 CFR § 164.520 ("Notice of privacy practices for protected health information").

whichever of the Defendants Plaintiff alleges he has a contract-based claim against.[3]

Plaintiff also alleges that, in the future, he will be required to spend time monitoring his accounts for fraudulent activity and will incur out-of-pocket costs for identity theft protection (Compl., ¶ 34). But according to the Complaint, Plaintiff has yet to spend a dime as a result of the Incident, and he does not plausibly allege he ever will. Plaintiff lastly adds that he has been harmed through anxiety, emotional distress, and loss of privacy (Compl. ¶ 34), but such a claim is not cognizable, nor is there a pleaded factual basis for such a claim in any event.

Therefore, as discussed more fully below, Plaintiff alleges neither the injury-in-fact nor traceability necessary for standing, nor the requisite amount in controversy for Class Action Fairness Act ("CAFA") subject matter jurisdiction. Alternatively, pursuant to Fed. R. Civ. P. 12(b)(6), all counts of the Complaint should be dismissed for failure to plead damage or injury and failure to plead other required elements of Plaintiff's causes of action.

ARGUMENT

I. THE COURT LACKS SUBJECT MATTER JURISDICTION.

Plaintiff has not pled any injury-in-fact that is traceable to the actions of Defendants. The Complaint should thus be dismissed under Rule 12(b)(1) for lack of standing under Article III of the United States Constitution. Additionally, no proper basis exists for this Court to exercise its jurisdiction on a diversity or CAFA basis.

A. Plaintiff Lacks Standing under Article III.

Plaintiff has the burden of establishing subject matter jurisdiction and the requisite standing to confer such jurisdiction. *See* Fed. R. Civ. P. 8(a)(1) (pleading must contain "a short

[3] There are limits to what a defendant can be forced to guess at when faced with an unintelligible and internally inconsistent pleading. On due process grounds alone, each defendant is entitled to "notice" sufficient to understand and respond to allegations in a complaint. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 545 (2007) (explaining the complaint must "give the defendant fair notice of what the ... claim is and the grounds upon which it rests" (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957))). Dismissal on these grounds alone is warranted on this record. *See Deal-Watkins v. Walters*, No. 2:13-CV-01808-GMN-VC, 2014 WL 7330941, at *1 (D. Nev. Dec. 19, 2014), *report and recommendation adopted,* No. 2:13-CV-01808-GMN, 2015 WL 1548946 (D. Nev. Apr. 7, 2015) ("'Prolix, confusing complaints' should be dismissed because 'they impose unfair burdens on litigants and judges.'" (quoting *Mc Henry v. Renne*, 84 F.3d 1172, 1179 (9th Cir. 1996))).

and plain statement of the grounds for the court's jurisdiction . . . "); *see also Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014). To establish standing, Plaintiff must allege an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (internal quotation marks omitted). The Supreme Court has emphasized that "[w]here, as here, a case is at the pleading stage, the plaintiff must 'clearly . . . allege facts demonstrating' each element [of the standing requirements]." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). A Rule 12(b)(1) motion challenging subject matter jurisdiction may be either facial or fact-based. *See White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). When, as here, the challenge is facial, it is based solely on the Complaint's allegations and any incorporated exhibits. *Id.* The well-pleaded factual allegations are assumed to be true for pleading purposes but remain subject to Plaintiff's burden of proof at summary judgment and trial. *Id.* Conclusory allegations of fact or law are not accepted as true. *Id.*

Here, Plaintiff claims he: (1) faces an increased risk of harm from fraud and identity theft; (2) may incur mitigation burdens and out-of-pocket expenses in the future; (3) somehow "overpaid" for contractually agreed cybersecurity services by Defendants that allegedly were represented to include adequate data security; and (4) suffered anxiety, emotional distress, and a loss of privacy. Compl., ¶¶ 33-37. None of these allegations, even when taken as true and afforded all reasonable inferences, establishes any "concrete and particularized" harm. Moreover, the Complaint fails to establish that any of the alleged "harm" is traceable to the Incident.

1. Potential Exposure of Plaintiff's Information Does Not Establish Substantial Risk of Future Injury.

To begin, Plaintiff has not adequately alleged standing based on a claimed increased risk of future identity theft or fraud resulting from the cyberattack. *See Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 409 (2013) (allowing for future injury standing under federal law only where plaintiffs allege either a "certainly impending" or "substantial risk" of future harm). The Ninth Circuit has twice analyzed standing based on an alleged increased risk of future identity fraud.

See In re Zappos, Inc., 888 F.3d 1020, 1027-28 (9th Cir. 2018); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010). In both cases, the court allowed for standing, but only because highly sensitive information was allegedly stolen with an impending risk of misuse. *See In re Zappos, Inc.*, 888 F.3d at 1023 (hackers intentionally targeted Zappos's servers and stole names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information from plaintiffs); *Krottner*, 628 F.3d at 1141 (laptop stolen containing Starbucks employee information, including names, addresses, and social security numbers; one of the three named plaintiffs alleged his bank had already notified him that "someone had attempted to open a new account in his name using his social security number").

District courts interpreting *Zappos* and *Krottner* have thus required plaintiffs to make specific allegations regarding how the data security incident at issue actually places them at an alleged increased risk of identity fraud, based both on the nature of the incident and on the type of information at issue. *See, e.g., Travis v. Assured Imaging LLC*, No. CV-20-00390-TUC-JCH, 2021 WL 1862446 at *6 (D. Ariz. May 10, 2021) (denying standing because "potential access" did not equate to "evidence the [Plaintiffs'] information was even stolen"); *Greenstein v. Noblr Reciprocal Exchange*, --- F.Supp.3d ---- 2022 WL 472183 at *3 (N.D. Cal. Feb. 14, 2022) (denying standing because "Plaintiffs allege only vague and unspecified harms" that are "speculative," such as the loss of privacy and a future risk of identity theft and fraud"); *Dearing v. Magellan Health Inc*., No. CV-20-00747-PHX-SPL, 2020 WL 7041059, at *3 (D. Ariz. Sept. 3, 2020), *reconsideration denied,* No. CV-20-00747-PHX-SPL, 2020 WL 7041048 (D. Ariz. Sept. 29, 2020) (denying standing based on an alleged increased risk of identity fraud where "Plaintiff fails to show her injury is 'certainly impending' or that there is a 'substantial risk that harm will occur.' Instead, her alleged risk is entirely speculative."); *see also In re Uber Tech., Inc. Data Sec. Breach Litig*., 2019 WL 6522843, at *4 (C.D. Cal. Aug. 19, 2019); *Jackson v. Loews Hotels, Inc.,* 2019 WL 6721637, at *3 (C.D. Cal. Jul. 24, 2019); *Ables v. Brooks Bros. Grp., Inc.*, 2018 WL 8806667, at *5 (C.D. Cal. Jun. 7, 2018); *Antman v. Uber Tech., Inc.*, 2018 WL 2151231, at *11 (N.D. Cal. May 10, 2018).

Plaintiff has not alleged any factual support for the allegation that his personal information was exposed as a result of a malicious actor targeting and acquiring that data. The Complaint contains facts indicating only that data concerning Plaintiff *might* have been exposed. For example, the Complaint admits that Plaintiff and proposed class members do not know "how unauthorized parties accessed their accounts, whether the information was encrypted or otherwise protected, how they learned of the Data breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many individuals were affected by the Data breach." Compl., ¶ 28. The Complaint simply argues "upon information and belief" that personally identifiable information was "stolen" or "obtained" by "cybercriminals," (Compl., ¶¶ 1, 5, 6, 32, 37, 40), yet admits that some or all of Plaintiff's information "may not have been involved in the Data breach" (Compl., ¶¶ 5, 36). Based solely on these speculations, Plaintiff concludes that "all of this personal information is *likely* for sale to criminals on the dark web" (Compl., ¶ 30) and "Plaintiff and fellow Class Members are more *likely* to unknowingly give away their sensitive personal information to other criminals" (Compl., ¶ 33 (emphasis added)). Plaintiff does not allege any factual support for the contention that his data was actually disclosed to or used by any third parties with malicious intent, and in fact, the lack of any pleaded cognizable damages after the Incident was discovered strongly suggests that no such malicious disclosure or use has occurred.

Plaintiff's failure to establish standing here is made even more categorical by the U.S. Supreme Court's recent ruling that "risk of future injury" alone simply cannot be equated to the "injury in fact" needed to establish standing in federal court. *See TransUnion LLC v. Ramirez,* No. 20-297, 2021 WL 2599472 (U.S. June 25, 2021) (no standing for class members who were not impacted by flawed information in credit reports that had not been disclosed or disseminated to others). As such, Plaintiff's elaborate theories about what may one day happen to him as a result of the Incident are non-starters to invoke the jurisdiction of the federal courts under the "case or controversy" requirement in Article III of the Constitution.

Plaintiff has not plausibly alleged future injury that is certainly impending, and, as stated above, any such showing would still not suffice to overcome the clear lack of standing in such

situations after the Supreme Court ruling in *TransUnion*.

2. Plaintiff Cannot Use Unspecified "Monitoring" Expenses to Manufacture Standing.

Given that Plaintiff has not plausibly alleged an imminent risk of future injury, he cannot instead allege that he may at some point in the future spend time "monitoring" for something that may never come to pass. *See* Compl., ¶ 34. Plaintiff does not allege that he has actually spent any time or money monitoring his credit, but even if he had, "plaintiff[s] cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Travis v. Assured Imaging LLC*, No. CV-20-00390-TUC-JCH, 2021 WL 1862446 at *9 (D. Ariz. May 10, 2021) (determining that monitoring costs were not sufficient to show Article III standing where there was not a sufficient risk of future harm); *see also Greenstein v. Noblr Reciprocal Exch.,* No. 21-CV-04537-JSW, 2022 WL 472183 at *6 (N.D. Cal. Feb. 15, 2022) (same). That is because "mitigation expenses do not qualify as actual injuries "in the absence of an imminent risk of harm." *Greenstein,* 2022 WL 472183 at *6; *see also Clapper*, 568 U.S. at 416 (one "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending"). Thus, Plaintiff's potential monitoring and or mitigation costs are also insufficient to establish the injury-in-fact necessary to confer standing.

3. Plaintiff Cannot Rely on "Benefit of the Bargain" Damages Without Support.

Plaintiff vaguely alleges that "Plaintiff and Class Members did not receive full benefit of the bargain they entered into" due to Defendants' supposed "failure to fulfill … data security protections." Compl. ¶ 85. Courts have uniformly rejected Plaintiffs' "benefit of the bargain" theory where, as here, the plaintiff fails to allege that this was a part of the bargain and that the price charged for goods or services includes a premium for enhanced security. *See, e.g., Birdsong v. Apple, Inc.*, 590 F.3d 955 (9th Cir. 2009) (rejecting plaintiff's benefit of the bargain theory, the court noted that the plaintiff failed to allege a different price charged to customers for purpose of security services); *see also McGee v. S-L Snacks Nat'l*, 982 F.3d 700, 706 (9th Cir. 2020) ("Absent some allegation that [Defendant] made false representations about [a products]

safety, [Plaintiff's] benefit of the bargain theory falls short."). Moreover, Plaintiff does not allege any injury from Defendants' alleged failure to provide the security measures for which Plaintiff claims to have paid a premium. Thus, even if "benefit of the bargain" damages could establish injury in fact, Plaintiff does not plausibly allege them and, as explained above, has left Defendants to speculate who exactly is being sued and for what, in violation of minimal pleading standards after *Iqbal* and *Twombly* and well short of Due Process norms and requirements.

4. Plaintiff's Emotional Distress, Anxiety, and Lack of Privacy Theories are Not Legally Cognizable.

Plaintiff lastly argues, without any factual support, that he suffered from anxiety, emotional distress, and lack of privacy. Compl., ¶ 34. Courts have rejected standing based on claimed emotional distress, anxiety, and loss of privacy following a data security incident, at least where the plaintiff cannot independently establish standing to sue based on an alleged increased risk of identity fraud. *See, e.g., Travis v. Assured Imaging LLC*, No. CV-20-00390-TUC-JCH, 2021 WL 1862446 at *6 (D. Ariz. May 10, 2021) (claims for emotional distress, anxiety, and loss of privacy in data breach action were not sufficient to confer standing); *In re Vtech Data Breach Litig.*, 2017 WL 2880102, at *5 n.6 (N.D. Ill. Jul. 5, 2017) (holding that "[w]here only an unspecified risk of future financial harm is alleged, emotional distress in the wake of a data security breach is insufficient to establish standing"); *Crusifilli v. Ameritas Life Ins. Corp., 2015 WL 1969176*, at *4 (D.N.J. Apr. 30, 2015) (same, noting "[c]ourts across the country have rejected 'emotional distress' as a basis for standing under similar circumstances"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 643-644 (3d Cir. 2011) (denying standing based on alleged emotional distress).

5. Plaintiff Fails to Plead Traceability.

In addition to failing to plead injury-in-fact, the Complaint does not plausibly allege any "harm" to Plaintiff traceable to the Incident. Plaintiff does not allege with any factual support that anyone has even gained access in fact to his information on Defendants' email accounts, let alone caused any actual damages. Plaintiff has simply alleged that he plans to undertake voluntary measures to monitor his accounts. The cases make clear that more is required. *Antman,*

2018 WL 2151231, at *23-24 (citations omitted); *see also Washington Env't. Council v. Bellon,* 732 F.3d 1131, 1141 (9th Cir. 2013); *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No. CV182970PSGGJSX, 2019 WL 6522843, at *5 (C.D. Cal. Aug. 19, 2019) (finding no traceable injury in breach case).

Moreover, the Supreme Court has ruled that the traceability requirement cannot be met with conjecture and hypothetical scenarios that could, in theory, be connected into a hypothetical chain of causation. *Clapper*, 568 U.S. 398 at 409. By equating "exposure" of servers to "access" to Plaintiff's data by unauthorized persons, the Complaint makes unwarranted assumptions regarding both injury and causation, not supported by any well-pleaded facts. This will not suffice. As the Supreme Court has repeatedly cautioned, "pleadings must be *something more than an ingenious exercise in the conceivable*." *United States v. SCRAP*, 412 U.S. 669, 688 (1973) (emphasis added).

B. Plaintiff Fails to Properly Plead Subject Matter Jurisdiction.

1. The Court Lacks Diversity Jurisdiction.

The diversity statute confers original jurisdiction on the federal district courts with respect to all civil actions where the matter in controversy "exceed[s] the value of $75,000," exclusive of interest and "all parties" have a "diverse residence." *Amerault v. Intelcom Support Servs., Inc*., 16 F. App'x 724, 725 (9th Cir. 2001) (citing 28 U.S.C. § 1332(a)). Although a low bar, a party invoking the jurisdiction of the federal court has the burden of proving that it appears to a reasonable probability that the claim is in excess of the statutory jurisdictional amount. *Id.* Here, Plaintiff cannot conceivably allege $75,000 in damages because Plaintiff cannot even claim that his data was ever disclosed to or used by any unauthorized third-party.[4]

2. The Court Lacks Jurisdiction Under CAFA.

Plaintiff also pleads that subject matter jurisdiction exists pursuant to CAFA. Compl. ¶ 11. CAFA, codified in part at 28 U.S.C. § 1332(d), confers federal jurisdiction over any class

[4] Defendants acknowledge the Court's July 12, 2022 Minute Order. (ECF No. 15.) Defendants do not contest the Court's finding of complete diversity of citizenship. Instead, as stated in the text, Defendants contend Plaintiff does not satisfy the amount in controversy requirement.

action involving: (1) "100 or more" class members, (2) an aggregate amount in controversy "exceeds $5,000,000," and (3) minimal diversity, *i.e.*, "any class member is a citizen of a state different from any defendant." *Serrano v. 180 Connect, Inc.*, 478 F.3d 1018, 1020-21 (9th Cir. 2007).

CAFA does not confer jurisdiction here because, among other things: (1) the matter in controversy does not "exceed $5,000,000," exclusive of interest and costs, under 28 U.S.C. § 1332(d)(2), and (2) there is no factual showing in the Complaint that the number of members of all proposed plaintiff classes in the aggregate is "100 or more" as required by 28 U.S.C. § 1332(d)(5)(B). Plaintiff proposes a class consisting of those individuals who have had their information "obtained" by criminals as a result of the Incident. *See* Compl., ¶ 40. As stated above, that number, on the face of the well pleaded allegations in the Complaint plus the Notice Letter incorporated therein, is zero. Additionally, Plaintiff identifies *no* actual damages from the Incident, to himself or anyone else, let alone damages exceeding $5 million.

The factual predicate for CAFA jurisdiction has simply not been pleaded. This is an additional reason the Court should dismiss the case for lack of subject matter jurisdiction.

II. THE COMPLAINT FAILS TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED.

In the alternative, the Complaint, consisting of four counts, should be dismissed pursuant to Rule 12(b)(6) for failure to state a claim. To survive a motion to dismiss for failure to state a claim pursuant to Rule 12(b)(6), a "complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The plausibility standard "asks for more than a sheer possibility that a defendant has acted unlawfully," and instead requires "enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of [the alleged misconduct]." *Iqbal*, 556 U.S. at 677; *Twombly*, 550 U.S. at 556.

A. Plaintiff Fails to Plead Legally Cognizable Damages.

Plaintiff brings causes of action for negligence, invasion of privacy by public disclosure of private facts and intrusion upon seclusion, breach of contract, and breach of implied contract.

Similar to the requirements for standing, the substantive causes of action pled in the Complaint includes actual injury as an essential element without which Plaintiff cannot state a cause of action. *See, e.g., Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc*., 125 Nev. 818, 824, 221 P.3d 1276, 1280 (2009) ("It is well established that to prevail on a negligence claim, a plaintiff must establish four elements: (1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages."); *Mizrahi v. Wells Fargo Home Mortg*., No. 2:09-CV-01387-RLH, 2010 WL 2521742, at *3 (D. Nev. June 16, 2010) (stating that "Nevada law requires the plaintiff in a breach of contract action to show: (1) the existence of a valid contract; (2) a breach by the defendant; and (3) *damage* as a result of the breach."); *Singer v. Las Vegas Athletic Clubs,* 376 F. Supp. 3d 1062, 1075 (D. Nev. 2019) ("To recover for the tort of intrusion, a plaintiff must prove the following elements: 1) an intentional intrusion (physical or otherwise); 2) on the solitude or seclusion of another; 3) that would be highly offensive to a reasonable person."). As addressed above, the allegations in the Complaint, even when read in a light most favorable to Plaintiffs, simply fail to allege the actual injury required to state a claim. *See Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1232 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021) (data breach case under Nevada law finding "that the 'imminent and certainly impending injury flowing from potential fraud and identity theft' and the continued risk to her personal data are too tenuous to constitute 'damages' as an element of plaintiff's claims" for negligence and breach of contract).

B. Plaintiff's Negligence Claim Fails.

1. Plaintiff Fails to Allege Causation or Damages.

Plaintiff brings a claim for negligence. Compl., ¶¶ 51-57. To state a cause of action for negligence, a plaintiff must demonstrate "(1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages." *Sanchez*, 125 Nev. at 824. Plaintiff's negligence claim fails to allege legally cognizable proximate cause and damages. *See Sanchez*, 125 Nev. at 824 (elements of negligence include legal causation and damages); *Pruchnicki*, 439 F. Supp. 3d at 1232 (because plaintiff did not allege sufficient facts that her data was misused she has not alleged damages). As explained above, Plaintiff provides no factual support for his allegation

that Plaintiff's personal identifying information was ever actually disclosed to any third-party. Notably, there is no allegation that images or data pertaining to Plaintiff were actually accessed or used by others, or that Plaintiff sustained any injury thereby.

For example, in *Pruchnicki v. Envision Healthcare*, the court found that "alleged injuries that stem from the danger of future harm are insufficient to support a negligence action, "and thus the "imminent and certainly impending injury flowing from potential fraud and identity theft" and "the continued risk to her personal data are too tenuous to constitute 'damages' as an element of plaintiff's claims." 439 F. Supp. 3d at 1232; *see also Aguilar* v. *Hartford Accident & Indem. Co.*, No. CV-18-8123-R, 2019 WL 2912861, at *2 (C.D. Cal. Mar. 13, 2019) ("[T]he loss of privacy engendered by an accidental data breach cannot satisfy the necessary damage element of a negligence claim, 'without specific factual statements that Plaintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges.'" (quoting *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 903 F.Supp.2d 942, 963 (S.D. Cal. Oct. 11, 2012)); *see also Galaria v. Nationwide Mut. Ins. Co.*, 998 F.Supp.2d 646, 658 (S.D. Ohio 2014), *rev'd and remanded on other grounds*, 663 F.App'x 384 (6th Cir. 2016) (rejecting the argument "that any time a plaintiff's PII has been exposed as a result of a data breach, he would [suffer any injury]—regardless of whether that PII is ever actually misused or the plaintiff ever suffers adverse consequences from the exposure."); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-CV-09600 RGK (Ex), 2015 WL 3916744 (C.D. Cal. June 15, 2015) (increased risk and lost time "too speculative to constitute cognizable injury"). Plaintiff's negligence claim should therefore be dismissed.

2. Plaintiff's Negligence Claim is Barred by the Economic Loss Doctrine.

"In Nevada, the economic loss doctrine bars negligent tort actions where the plaintiff seeks to recover only economic loss." *Fuoroli v. Westgate Planet Hollywood Las Vegas, LLC,* No. 2:10-CV-2191-JCM-GWF, 2011 WL 1871236, at *3 (D. Nev. May 16, 2011); *see also Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 125 Nev. 66, 73, 206 P.3d 81, 86 (2009) ("[T]his court has concluded that the doctrine bars unintentional tort actions when the plaintiff

seeks to recover 'purely economic losses.'"). Put simply, "unless there is personal injury or property damage, a plaintiff may not recover in negligence for economic losses." *Terracon Consultants W., Inc.*, 125 Nev. at 74.

Courts applying Nevada law in data breach cases have held that the economic loss doctrine bars negligence-based claims. *Affinity Gaming v. Trustwave Holdings, Inc.*, No. 2:15-CV-02464-GMN-PAL, 2016 WL 5799300, at *6 (D. Nev. Sept. 30, 2016) (dismissing gross negligence claim under economic loss doctrine); *In re Zappos.com, Inc.*, No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (stating that "the Court is compelled to agree with Defendant that the economic loss doctrine bars recovery in negligence in this case.").

As discussed above, Plaintiff does not allege any facts, whatsoever, to plausibly allege he was injured by the Incident. But, even if he was injured, his injuries would be solely economic. Plaintiff did not and cannot allege that she suffered personal injury. And diminution in the value of personal information is not the type of "property damage" contemplated by the economic loss doctrine. *See, e.g., In re TJX Companies Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009), *as amended on reh'g in* part (May 5, 2009) (affirming dismissal of negligence claims under the economic loss doctrine and stating that, although "[e]lectronic data can have value and the value can be lost,…the loss here is not a result of physical destruction of property" and, therefore, is purely economic). Plaintiff's negligence claim is barred by Nevada's economic loss doctrine and should be dismissed.

C. Plaintiff's Intrusion Upon Seclusion Claim Fails.

Plaintiff alleges a claim based on "invasion of privacy" and "intrusion upon seclusion." Compl. ¶¶ 58-62. Nevada law applies the Second Restatement of Torts test to intrusion upon seclusion claims, which requires a plaintiff to prove three elements: "1) an intentional intrusion (physical or otherwise); 2) on the solitude or seclusion of another; 3) that would be highly offensive to a reasonable person." *Singer*, 376 F. Supp. 3d at 1075.

First, Plaintiff never alleges that Defendants committed any intrusion at all, let alone an intentional one. Plaintiff's effort to shift blame for the alleged intrusion from the alleged "hackers" to Defendants is improper and unsupported by the factual allegations in the Complaint.

Second, Plaintiff never pleads facts supporting any intrusion at all. As addressed above, Plaintiff bases each of his claims on potential access to his data and nothing more. This is insufficient to state a claim under Nevada law for intrusion upon seclusion.

Second, Plaintiff does not even allege that Defendants' conduct "would be highly offensive, nor does Plaintiff allege any intrusion or unauthorized use of Plaintiff's data by Defendants. Indeed, there is no allegation of any unauthorized use of Plaintiff's data at all—let alone use resulting in damage to Plaintiff. Without more, Plaintiff fails to state a claim for intrusion upon seclusion.

D. Plaintiff's Breach of Contract Claims Fail.

Plaintiff purports to allege breach of contract (Count III) and breach of implied contract (Count IV). Compl. ¶¶ 63-87. "Nevada law requires the plaintiff in a breach of contract action to show: (1) the existence of a valid contract; (2) a breach by the defendant; and (3) damage as a result of the breach." *Mizrahi v. Wells Fargo Home Mortg*., No. 2:09-CV-01387-RLH, 2010 WL 2521742, at *3 (D. Nev. June 16, 2010). In addition to be being indecipherable and hence subject to dismissal on that basis alone, as stated above, both claims fail because of the lack of a contract, let alone a lack of a breach or resulting damages.

1. Plaintiff Fails to Plead an Offer or Acceptance.

First, Plaintiff fails to plead offer and acceptance. To create an enforceable contract, there must be an "offer and acceptance, meeting of the minds, and consideration." *May v. Anderson,* 121 Nev. 668, 672 (2005). "Express and implied contracts differ in the manner that sets forth the terms of the agreement—the terms of an express contract are stated in words while those of an implied contract are manifested by conduct." *Mizrahi,* 2010 WL 2521742, at *3. To pursue an implied contract theory, however, the plaintiff "must elaborate upon the nature and scope of the implied contract in the pleadings…." *In re Anthem, Inc. Data Breach Litig.*, 162 F.Supp.3d 953, 982–83 (N.D. Cal. 2016). Specifically, the plaintiff must allege facts sufficient to support a finding that "the parties intended to contract and promises were exchanged, the general obligations for which must be sufficiently clear." *Risinger v. SOC LLC,* 936 F.Supp.2d 1235, 1247 (D. Nev. 2013).

But Plaintiff does not provide a copy of the supposed contract or any basis for the existence of a contract, express or implied. Plaintiff's breach of contract claims are merely based on an allegation that Defendants were supposed to take some undefined action, based on some undefined implied contractual term, but somehow failed to do so. Such an allegation does not make the "general obligations … sufficiently clear." As such, Plaintiff's breach of contract and breach of implied contract claims should be dismissed.

At best, Plaintiff attempts to concoct a breach of contract claim from Defendants' data breach notification letter. Compl., ¶ 79. Plaintiff cannot plead that the breach notification letter was a contract, as it was merely an informational resource and did not even exist until after the Incident. Likewise, an offer is not accepted until a communication of acceptance is made. 6:61. Time of formation of contract, 2 Williston on Contracts § 6:61 (4th ed.). Yet Plaintiff does not allege that he took any action to "accept" statements by one or more Defendants in the Notice Letter or otherwise. Nor could he, as there was nothing "offered."

2. Plaintiff Fails to Plead Consideration.

Second, Plaintiff fails to allege consideration. Claims for breach of both express and implied contracts "must be supported by consideration." *Helash v. Ballard*, 638 F.2d 74, 75 (9th Cir. 1980). Plaintiff does not allege any consideration was provided. This claim fails as a matter of law. Plaintiff should not be allowed to shoehorn passages from the Notice Letter or other sources into a contractual relationship.[5] Because Plaintiff fails to plead the basic elements of a contract, these counts must be dismissed.

CONCLUSION

For the reasons stated above, the Complaint should be dismissed.

[5] Courts in other data breach cases have expressly rejected this tactic. *See, e.g.*, *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 980 (N.D. Cal. 2016) (plaintiffs failed to allege "the privacy notices or public website statements were part of or were incorporated by reference into Plaintiffs' contracts with the Anthem Defendants.").

Dated: July 29, 2022

Respectfully submitted,

SANTORO WHITMIRE

/s/ James E. Whitmire
James E. Whitmire
Nevada State Bar No. 6533
10100 W. Charleston Blvd., Suite 250
Las Vegas, Nevada 89135
Telephone: (702) 948-8771
E-mail: jwhitmire@santoronevada.com

POLSINELLI PC

John C. Cleary
(*pro hac vice* forthcoming)
600 Third Avenue, 42nd Floor
New York, New York 10016
Telephone: (212) 413-2837
E-mail: john.cleary@polsinelli.com

Mark A. Olthoff
(*pro hac vice* forthcoming)
E-mail: molthoff@polsinelli.com
Catherine A. Green
(*pro hac vice* forthcoming)
E-mail: cgreen@polsinelli.com
900 W. 48th Place, Suite 900
Kansas City, Missouri 64112-1895
Telephone: (816) 753-1000

Attorneys for Defendants MX Holdings US, Inc., CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on July 29, 2022, this document was filed through the Electronic Case Filing system of the United States District Court for the District of Nevada and will be served electronically by the Court to the Registered Participants identified in the Notice of Electronic Filing (NEF).

/s/ James E. Whitmire
James E. Whitmire

Exhibit Index	
Exhibit A	Template Notice Letter
Exhibit B	*Dearing v. Magellan Health Inc.*, Case No. 2:20-cv-00747, ECF No. 31 (D. Ariz. Sept. 29, 2020)
Exhibit C	*Agans et al. v. Uber Techs., Inc.*, Case No. 2:18-cv-02970-PSG-GJS, ECF No. 72 (C.D. Cal. Aug. 19, 2019)

Exhibit A – Template Notice Letter

MX HOLDINGS US, INC.

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

RE: NOTICE OF DATA BREACH

On behalf of MX Holdings US, Inc. and its subsidiaries, including CFP Fire Protection, Inc., COSCO Fire Protection, Inc., and Firetrol Protection Systems, Inc., we are writing to inform you of a recent incident that may have resulted in the temporary exposure of some of your personal information. We value the trust you place in our organization. We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On or about October 28, 2021, we observed suspicious activity within our email system. We immediately engaged a third-party forensic security firm to investigate the issue and confirm the security of our computer systems. This investigation determined that an unauthorized third party was able to temporarily access several email accounts. Additionally, we promptly retained a specialized document review vendor to examine the email accounts to determine whether any personal information was contained in the accounts.

What Information Was Involved? On or about April 5, 2022, we determined that the relevant email accounts contained certain personal information. That information varied by individual, but may have included your name, date of birth, Social Security number, driver's license number, passport number, financial account number, and/or limited medical information.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect yourself.

Finally, although we are not aware of any instances of fraud or identity theft resulting from this incident, in an abundance of caution, we are offering a complimentary one-year membership of *my*TrueIdentity online Credit Monitoring by TransUnion. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. *my*TrueIdentity online Credit Monitoring is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and *my*TrueIdentity online Credit Monitoring, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. In addition to enrolling in the complimentary identity theft protection and credit monitoring service, you can find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call 844-571-2173 from 6:00 AM - 6:00 PM Pacific, Monday through Friday.

Sincerely,

Keith Fielding

TransUnion

1. Activation Code: <<Activation Code>>

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12/24>> months provided by TransUnion Interactive, asubsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code

<<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<<Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<12/24>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit reportonline, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected <<RI Count>> Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Washington, DC Residents: Washington, DC residents can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

Exhibit B – *Dearing v. Magellan Health Inc.*

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Carol Dearing, Plaintiff, vs. Magellan Health Incorporated, et al., Defendants.	No. CV-20-00747-PHX-SPL **ORDER**

Before the Court is Defendant's Motion to Dismiss pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(1) and 12(b)(6). (Doc. 15) For the following reasons, the Motion will be granted.[1]

I. BACKGROUND

This case arises out of a data breach that occurred on May 28, 2019. (Doc. 1 at ¶ 4) Defendant Magellan Health, Incorporated ("Defendant") discovered on July 5, 2019, that one of its employees fell for a phishing scheme that allowed a third party to access his or her email account. (Doc. 1 at ¶¶ 3-4) Defendant notified its customers of the breach on or about November 8, 2019. (Doc. 1 at ¶ 3) On April 17, 2020, Plaintiff Carol Dearing ("Plaintiff") filed a complaint in this Court, on behalf of herself and all others similarly situated (Doc. 1 at ¶ 75), alleging negligence, negligence per se, breach of implied contract,

[1] Because it would not assist in resolution of the instant issues, the Court finds the pending motion is suitable for decision without oral argument. *See* LRCiv. 7.2(f); Fed. R. Civ. P. 78(b); *Partridge v. Reich*, 141 F.3d 920, 926 (9th Cir. 1998).

unjust enrichment, and violations of the Arizona Consumer Fraud Act. (Doc. 1 at 27-37) On May 13, 2020, Defendant filed a motion to dismiss under Rule 12(b)(1) and Rule 12(b)(6). (Doc. 15) The motion is fully briefed and ready for review. (Docs. 15, 16, 21, 22)

II. LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(1) "allows litigants to seek the dismissal of an action from federal court for lack of subject matter jurisdiction." *Kinlichee v. United States*, 929 F. Supp. 2d 951, 954 (D. Ariz. 2013) (quotation omitted). "Allegations raised under Rule 12(b)(1) should be addressed before other reasons for dismissal because if the complaint is dismissed for lack of subject matter jurisdiction, other defenses raised become moot." *Kinlichee*, 929 F. Supp. 2d at 954. "A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may attack either the allegations of the complaint as insufficient to confer upon the court subject matter jurisdiction, or the existence of subject matter jurisdiction in fact." *Renteria v. United States*, 452 F. Supp. 2d 910, 919 (D. Ariz. 2006)); *Edison v. United States*, 822 F.3d 510, 517 (9th Cir. 2016). "When the motion to dismiss attacks the allegations of the complaint as insufficient to confer subject matter jurisdiction, all allegations of material fact are taken as true and construed in the light most favorable to the nonmoving party." *Renteria*, 452 F. Supp. 2d at 919. "When the motion to dismiss is a factual attack on subject matter jurisdiction, however, no presumptive truthfulness attaches to the plaintiff's allegations, and the existence of disputed material facts will not preclude the trial court from evaluating for itself the existence of subject matter jurisdiction in fact." *Id*. "A plaintiff has the burden of proving that jurisdiction does in fact exist." *Id*.

III. DISCUSSION

Defendant argues that the Complaint should be dismissed because Plaintiff failed to establish standing under Rule 12(b)(1) and failed to state a claim upon which relief may be granted under Rule 12(b)(6). (Doc. 16 at 8, 12) Specifically, Defendant asserts that Plaintiff lacks Article III standing because she has failed to establish an injury-in-fact.

"Under Article III, § 2 of the Constitution, federal courts have jurisdiction over a

dispute only if it is a case or controversy." *See Cetacean Cmty. v. Bush*, 386 F.3d 1169, 1174 (9th Cir. 2004). "To state a case or controversy under Article III, a plaintiff must establish standing." *Arizona Christian School Tuition Organization v. Winn*, 563 U.S. 125, 133 (2011); *see also Hein v. Freedom from Religion Found., Inc.*, 551 U.S. 587, 597–98 (2007) (Article III standing limits judicial review to cases and controversies). "The constitutional requirement of standing has three elements: (1) the plaintiff must have suffered an injury-in-fact—that is, a concrete and particularized invasion of a legally protected interest that is actual or imminent, not conjectural or hypothetical; (2) the injury must be causally connected—that is, fairly traceable—to the challenged action of the defendant and not the result of the independent action of a third party not before the court; and (3) it must be likely and not merely speculative that the injury will be redressed by a favorable decision by the court." *Catholic League for Religious and Civil Rights v. City and County of San Francisco*, 624 F.3d 1043, 1049 (9th Cir. 2010) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992); *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 475–76 (1982)).

The plaintiff bears the burden of establishing the existence of a justiciable case or controversy, and "'must demonstrate standing for each claim he seeks to press' and 'for each form of relief' that is sought." *Davis v. Federal Election Comm'n*, 554 U.S. 724, 734, (2008) (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352, (2006)). "A plaintiff must establish standing with the 'manner and degree of evidence required at the successive stages of the litigation.'" *Carrico v. City and County of San Francisco*, 656 F.3d 1002, 1006 (9th Cir. 2011) (quoting *Lujan*, 504 U.S. at 561). "[A]t the pleading stage, the plaintiff must clearly . . . allege facts demonstrating each element." *Spokeo, Inc. v. Robins*, —— U.S. ——, 136 S.Ct. 1540, 1547 (2016) (internal quotations omitted).

Here, Plaintiff's asserted injuries are as follows: Defendant's data breach (a) caused "imminent and impending injury arising from the increased risk of fraud and identity theft"; (b) caused Plaintiff to spend time and money monitoring her accounts, contacting credit bureaus and credit card companies, and otherwise attempting to protect her information;

(c) caused money to be paid to Defendant that would not have been paid had Defendant disclosed that it lacked sufficient "data security practices" to safeguard customers' protected health information ("PHI") and personally identifiable information ("PII") from theft; and (d) caused damages and diminution in value of Plaintiff's PHI and PII. (Doc. 1 at 20–21) Upon review, the Court finds that Plaintiff's pleadings do not allege facts that constitute an injury-in-fact that is a "concrete and particularized invasion of a legally protected interest that is actual or imminent" and "not conjectural or hypothetical." *See Lujan*, 504 U.S. at 560.

A. Risk of fraud and identity theft

Plaintiff alleges that she is at risk of an imminent and impending injury arising from the risk of fraud and identity theft caused by the data breach. (Doc. 1 at 20–21) In order to prove an injury-in-fact in a data breach case, a plaintiff must show the harm has already occurred, there is a "substantial risk that the harm will occur," or that the threatened injury is "certainly impending." *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023 (9th Cir. 2018); *see also Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010). There must be "a credible threat of real and immediate harm stemming from the theft of [data]." *Krottner*, 628 F.3d at 1143. The plaintiff need not suffer data misuse or identity theft before he or she has an injury for standing purposes, but the data must be actually stolen and taken in a "manner that suggests it will be misused." *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214–16 (N.D. Cal. 2014). Plaintiff cites *Adobe* to support her allegations that she need not suffer identity theft before she brings her suit, but neglected to acknowledge, as Defendant did in its response, that the *Adobe* case is distinguishable from the case at hand. In *Adobe*, there was evidence the hackers stole the customer data, used Adobe systems to decrypt customer credit cards, and used the stolen data to discover vulnerabilities in Adobe products. *Id.* The PII in that case was deliberately targeted. *See also Zappos.com*, 888 F.3d at 1027–28 (plaintiffs showed evidence their information was stolen and used to take over their email accounts and identities); *Krottner*, 628 F.3d at 1143 (a hacker stole an employee laptop containing sensitive PII and retained possession of the

laptop and data); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855 (N.D. Cal. 2011) (possible injury when a confirmed hacker accessed the defendant's database and copied email and social networking logins of users). Other courts have found no injury when there was no theft or targeting of information. *See Stasi v. Inmediata Health Grp. Corp.*, No. 19CV2353 JM (LL), 2020 WL 2126317, at 6 (S.D. Cal. May 5, 2020) (finding no injury despite a breach that made the plaintiffs' PII and PHI temporarily available online when there was no evidence the information was copied, saved, or misused).

Here, Plaintiff's PII and PHI did not appear to be deliberately targeted, and there is no evidence the information was even stolen. Plaintiff's complaint includes the notice Defendant sent to affected parties, which stated that the phisher may have seen emails in the employee's account while attempting to send out spam. (Doc. 1 at 6–7) These emails contained information such as names, social security numbers, health plan ID numbers, health plan names, healthcare providers, and drug names; *i.e.*, PHI and PII. (Doc. 1 at 7) The notice also stated Defendant had no proof the phisher actually saw any emails in the account. (Doc. 1 at 6) Even if he or she did see the emails, his or her intent was to send spam using a Defendant employee email address. Furthermore, upon discovering the breach, Defendant locked the employee's account and prevented the phisher from accessing it further. Plaintiff even includes that information in her complaint and fails to show the phisher had previously obtained or is currently in possession of her information and/or the information of other customers. (Doc. 1 at 6–7) As a result, Plaintiff fails to show her injury is "certainly impending" or that there is a "substantial risk that harm will occur." Instead, her alleged risk is entirely speculative.

B. Time and money spent

Plaintiff alleges that she has spent time and money monitoring her accounts and contacting credit bureaus and credit card companies to protect her information. However, when a risk of future harm is speculative, a plaintiff cannot "manufacture standing by choosing to make expenditures based on hypothetical harm that is not certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 401 (2013). Defendant mentions

the *Clapper* holding in its motion to dismiss (Doc. 15 at 12) and Plaintiff fails to address it in her response. (Doc. 21) Furthermore, Defendant offered Plaintiff free personal information protection immediately after the breach, including credit monitoring, a reimbursement policy, and a fully managed ID theft recovery service. Plaintiff need not have spent any time or money at all, but she chose to make those expenditures. The Northern District of California encountered a similar contention in *Ruiz v. Gap, Inc.*, in which the plaintiff sought recovery of costs incurred over more than a year while monitoring his accounts and credit cards. 622 F. Supp. 2d 908, 915 (N.D. Cal. 2009), aff'd, 380 F. App'x 689 (9th Cir. 2010). The court found (1) there was no evidence of significant exposure of the plaintiff's personal information and no evidence that he was a victim of identity theft and (2) plaintiff's contention that the monitoring was necessary held little weight because he had the opportunity to receive free credit monitoring from the defendant and declined. *Id.* Therefore, the court found the plaintiff did not meet his evidentiary burden.

Relatedly, the Court now finds that Plaintiff's unnecessary expenditures are not an injury giving rise to standing.

C. Money conferred

Plaintiff is a member of TennCare, Tennessee's state-sponsored Medicaid program (Doc. 1 at 2, ¶ 1). In her Complaint, Plaintiff alleges that Defendant received payment based on contracts with TennCare and other Medicaid providers to manage and administer pharmaceutical benefits. (Doc. 1 at 2). Plaintiff further asserts that because of the breach in security, Defendant should not be "permitted to retain the money belonging to Plaintiff and Class Members" that was paid under the contract. (Doc. 1 at ¶ 126)

Defendant asserts that Plaintiff never paid it any money. (Doc. 16 at 9) As a result, Defendant argues Plaintiff cannot maintain an injury. (Doc. 16 at 9) Plaintiff argues she suffered damage as a result of Defendant's receipt of payment under the contract based on her status as a third-party beneficiary and can recover because her PII and PHI was exposed. (Doc. 21 at 10–12) Defendant never addresses the third-party beneficiary

argument in their pleadings, instead glossing over it by realleging Plaintiff never paid them any money. (Doc. 22 at 6)

"To sue as a third-party beneficiary of a contract, the third party must show that the contract reflects the express or implied intention of the parties to the contract to benefit the third party." *Klamath Water Users Protective Ass'n v. Patterson*, 204 F.3d 1206, 1211 (9th Cir. 1999), *opinion amended on denial of reh'g*, 203 F.3d 1175 (9th Cir. 2000). The intended beneficiary does not need to be mentioned in the contract, but "must fall within a class clearly intended by the parties to benefit from the contract." *Id.* "One way to ascertain such intent is to ask whether the beneficiary would be reasonable in relying on the promise as manifesting an intention to confer a right on him or her." *Id.* (*citing* Restatement § 302(1)(b) cmt. d).

Here, Plaintiff states that by entering the contract with Defendant, TennCare expected Defendant to safeguard their members' PII and PHI. (Doc. 1 at ¶123–125)[2] The Northern District of California has recognized a third-party beneficiary cause of action for individuals unnamed in a contract who relied on the parties to safeguard their PII. *See In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *18–19 (N.D. Cal. May 27, 2016). However, even if Plaintiff may have asserted a viable third-party beneficiary claim, and even if there was a breach of the contract between Defendant and TennCare, Plaintiff has not alleged any cognizable harm as a result of the breach for the foregoing reasons. *See* supra § III(A)–(B). "In order to state a claim for breach of contract, a plaintiff must allege the existence of a contract between the plaintiff and defendant [or prove she is a third party beneficiary], a breach of the contract by the defendant, *and* resulting damage to the plaintiff." *Snyder v. HSBC Bank, USA, N.A.*, 873 F. Supp. 2d 1139, 1148 (D. Ariz. 2012) (internal citations omitted) (emphasis added). Plaintiff failed to allege damages because she failed to show her information was stolen or

[2] Because the Court did not consider the contract between TennCare and Magellan Medicaid Administration, Inc., the court finds the Defendant's Request for Judicial Notice (Doc. 17) to be moot.

misused. Moreover, Plaintiff has not cited any cases to the contrary, instead citing to cases she claims prove that there need not be a contractual relationship to give rise to standing. The Court finds those cases to be inapposite. *See Lujan*, 504 U.S. 555; *Raines v. Byrd*, 521 U.S. 811 (1997); *Elk Grove Unified School Dist. v. Newdow*, 542 U.S. 1 (2004). (Doc. 21 at 12) None of these cases involved contractual disputes or injuries to third-party beneficiaries arising out of breach of contract, and thus the courts did not consider the question of whether a contractual relationship was required. Regardless, there must be an injury as a result of the breach of contract, and here there was no injury to Plaintiff.

D. Diminution in value to PHI and PII

Finally, Plaintiff alleges that her PHI and PII are now damaged and have diminished in value as a result of the hack. (Doc. 1 at 20–21) She does not provide a basis for this allegation, other than the notice, which does not support the facts asserted. *See* supra §(A).

Although not yet addressed by the 9th Circuit or District of Arizona, the Court agrees with decisions from the Northern District of California, which have been unwilling to find standing based solely on a theory that the value of a plaintiff's PII has been diminished. Thus, a plaintiff must assert another cognizable injury beyond diminution in value to support such a claim. *See In re iPhone Application Litigation*, 844 F. Supp. 2d 1040 (N.D. Cal 2012) (injury arose from a violation of the Wiretap Act *and* accessing or tracking personal information, which is an independent basis "beyond theoretical allegations that personal information has independent economic value"); *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013) (no injury where PII was diminished in value without a showing that the plaintiff had attempted or would later attempt to profit off his PII's value, and without showing of other injury). Diminution in value is not on its own a sufficient injury to establish Article III standing. Here, because Plaintiff has not asserted any other sufficient injuries, Plaintiff has not established Article III standing.

///

///

IV. CONCLUSION

For the foregoing reasons,[3] the Court finds that Plaintiff lacks standing to bring this claim. Accordingly,

IT IS ORDERED that Defendant's Motion to Dismiss (Doc. 15) is **granted.**

IT IS FURTHER ORDERED that Plaintiff's Complaint (Doc. 1) is **dismissed** with prejudice for lack of subject matter jurisdiction.

IT IS FURTHER ORDERED that Defendant's Request for Judicial Notice (Doc. 17) is **denied as moot**.

IT IS FURTHER ORDERED that the Clerk of Court shall terminate this action.

Dated this 3rd day of September, 2020.

Honorable Steven P. Logan
United States District Judge

[3] Because the Court finds the Plaintiff lacks standing in this case, it need not address Defendant's Rule 12(b)(6) arguments because this Court does not have subject matter jurisdiction. *See Kinlichee v. United States*, 929 F. Supp. 2d 951, 954 (D. Ariz. 2013).

Exhibit C – *Agans et al. v. Uber Techs., Inc.*

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

#47

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

Present: The Honorable	Philip S. Gutierrez, United States District Judge	
Wendy Hernandez		Not Reported
Deputy Clerk		Court Reporter
Attorneys Present for Plaintiff(s):		Attorneys Present for Defendant(s):
Not Present		Not Present

Proceedings (In Chambers): The Court GRANTS Defendant's motion to dismiss

Before the Court is Defendant Uber Technologies, Inc.'s ("Defendant" or "Uber") motion to dismiss Plaintiff Steven Agans ("Plaintiff" or "Agans"). *See* Dkt. # 47 ("*Mot.*"). Plaintiff opposes the motion, *see* Dkt. # 63 ("*Opp.*"), and Defendant replied, *see* Dkt. # 66 ("*Reply*"). The Court heard oral argument on the matter on August 19, 2019. Having considered the moving papers and arguments made at the hearing, the Court **GRANTS** the motion.

I. Background

A. Factual Background

Uber is a technology company that offers a smartphone application (the "Uber App") that connects riders looking for transportation to drivers based on their location. *See First Amended Complaint*, Dkt. # 39 ("*FAC*"), ¶¶ 2, 13. Plaintiff used the Uber App as a driver from late 2013 through early 2014. *Id.* ¶ 5.

Uber requires its users to provide personally identifiable information ("PII") to use the App. *Id.* ¶¶ 14–15. PII that Uber collects includes, among other things, names, addresses, email addresses, credit card numbers, and driver's license numbers for its drivers. *See id.* ¶¶ 14–15, 22, 26.

In October 2016, the users' PII was subject to a data security breach ("2016 Data Breach"). *Id.* ¶ 1. Although Uber learned about the 2016 Data Breach by November 2016, it did not reveal it for a full year. *See id.* ¶¶ 17–18. On November 21, 2017, news reports regarding

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

the 2016 Data Breach surfaced, publicly exposing its details for the first time. *See id.* Uber subsequently issued several statements on its website, confirming much of what was published in the news reports. *Id.* ¶ 25. According to the news reports, two hackers accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained to discover an archive of Uber's rider and driver information. *Id.* ¶ 21. The hackers then emailed Uber asking for money. *Id.* Uber paid the hackers $100,000 "in an effort to cover up the 2016 Data Breach." *Id.* ¶ 19.

The compromised data included the names, email addresses, and mobile phone numbers of 50 million riders and 7 million drivers, including some 600,000 U.S. driver's license numbers. *See id.* ¶¶ 22, 26. It was further reported that no social security numbers, credit card information, trip location details, or other data were taken. *See id.* ¶ 22.

Plaintiff alleges that he suffered injuries from the 2016 Data Breach, including "time and expenses related to monitoring [his] financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, invasion of [his] privacy, and loss of value of [his] Private Information." *Id.* ¶ 43.

B. Procedural Background

On November 22, 2017, Plaintiffs Steven Agans and Audrey Diaz Sanchez filed suit in the Northern District of California against Uber, asserting jurisdiction under the Class Action Fairness Act of 2005. *See* Dkt. # 1. In February 2018, Plaintiffs amended the complaint and replaced Sanchez with Charity Bustamante. *See generally FAC.*

Agans and Bustamante bring this action for themselves and on behalf of a class of "[a]ll persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2016." *Id.* ¶ 55. Alternatively, they bring the action on behalf of sub-classes of California and Georgia users. *Id.* ¶¶ 56–57.

The First Amended Complaint ("FAC") asserts the following causes of action:

First Cause of Action: Violation of California Customer Records Act, Cal. Civ. Code §§ 1798.81.5 & 1798.82. *Id.* ¶¶ 67–81.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

Second Cause of Action: Violation of California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200 et seq. *Id.* ¶¶ 82–93.

Third Cause of Action: Negligence. *Id.* ¶¶ 94–104.

Fourth Cause of Action: Violation of Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-390 et seq. *Id.* ¶¶ 105–11.

Fifth Cause of Action: Violation of California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750 et seq. *Id.* ¶¶ 112–26.

In April 2018, the Judicial Panel on Multidistrict Litigation consolidated the proceedings under the heading *In re: Uber Technologies, Inc., Data Security Breach Litigation*, and transferred the case to this Court. *See* Dkts. # 55. In April 2019, the Court granted Defendant's motion to compel arbitration of Bustamante's claims. *See* Dkt. # 67.

Defendant now moves to dismiss Plaintiff's claims pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). *See generally Mot.*

II. Legal Standard

Federal courts have limited jurisdiction and therefore only possess power authorized by Article III of the United States Constitution and statutes enacted by Congress. *See Bender v. Williamsport Area Sch. Dist.*, 475 U.S. 534, 541 (1986). Thus, federal courts cannot consider claims for which they lack subject matter jurisdiction. *See Wang ex rel. United States v. FMC Corp.*, 975 F.2d 1412, 1415 (9th Cir. 1992).

Federal Rule of Civil Procedure 12(b)(1) provides for a party, by motion, to assert the defense of "lack of subject-matter jurisdiction." This defense may be raised at any time, and the Court is obligated to address the issue sua sponte. *See* Fed. R. Civ. P. 12(h)(1) (providing for waiver of certain defenses but excluding lack of subject matter jurisdiction); *Grupo Dataflux v. Atlas Global Grp.*, 541 U.S. 567, 571 (2004) ("Challenges to subject-matter jurisdiction can of course be raised at any time prior to final judgment."); *Moore v. Maricopa Cty. Sheriff's Office*, 657 F.3d 890, 894 (9th Cir. 2011) ("The Court is obligated to determine *sua sponte* whether it has subject matter jurisdiction."). The plaintiff bears the burden of establishing that subject

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

matter jurisdiction exists. *See United States v. Orr Water Ditch Co.*, 600 F.3d 1152, 1157 (9th Cir. 2010). If the Court finds that it lacks subject matter jurisdiction at any time, it must dismiss the action. *See* Fed. R. Civ. P. 12(h)(3).

A Rule 12(b)(1) jurisdictional attack may be facial or factual. *See White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). In a facial attack, as is the case here, the challenging party asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction. *See Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction. *See id*.

III. Discussion

Defendant contends that the Court should dismiss Plaintiff's claims because he lacks Article III standing to bring suit.[1] *See generally Mot.*

A plaintiff must "have 'standing' to challenge the action sought to be adjudicated in the lawsuit." *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982). The "irreducible constitutional minimum" of Article III standing has three elements: (1) "the plaintiff must have suffered an injury in fact—an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent"; (2) "there must be a causal connection between the injury and the conduct complained of"; and (3) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992) (internal quotation marks omitted). The plaintiff, as the party invoking federal jurisdiction, has the burden of establishing these elements. *See id.* at 561. Article III standing bears on the court's subject matter jurisdiction and is therefore subject to challenge under Federal Rule of Civil Procedure 12(b)(1). *See Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011).

In a class action, the named plaintiff "must allege and show that [he] personally ha[s] been injured, not that injury has been suffered by other, unidentified numbers of the class to which they belong and which they purport to represent." *Warth v. Seldin*, 422 U.S. 490, 502

[1] Because the Court concludes that Agans has failed to establish standing, it does not reach Defendant's arguments under Federal Rule of Civil Procedure 12(b)(6).

(1975). If the named plaintiff cannot establish the requisite case or controversy with the defendant, "none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974).

Here, Uber argues that Plaintiff lacks Article III standing to pursue his claims because the FAC fails to sufficiently plead an injury-in-fact or a causal connection between the injury and Uber's alleged misconduct. *See Mot.* 6:1–2.

A. Injury-in-Fact

i. Increased Risk of Fraud and Identity Theft

Uber first argues that Plaintiff's primary claim of injury—that he now faces "an increased, imminent risk of fraud and identity theft," *FAC* ¶ 43—is too "conjectural" and "hypothetical" to establish standing. *Mot.* 6:5–7 (quoting *Lujan*, 504 U.S. at 560).

For a plaintiff to recover for a threatened future injury, it is not enough to allege that a future injury is possible; rather, he must show that the threatened injury is "certainly impending." *In re Zappos.com, Inc. (Zappos)*, 888 F.3d 1020, 1026 (9th Cir. 2018) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013)). The Ninth Circuit has repeatedly held that the same principle applies in the context of data breaches. For instance, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the plaintiffs were Starbucks employees whose names, addresses, and social security numbers were on a laptop that was stolen from Starbucks. *Id.* at 1140. The Ninth Circuit found that the plaintiffs "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data," *id.* at 1143, even though their data had not yet been misused. However, were the plaintiffs' allegations "more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—[it] would [have found] the threat far less credible." *Id.*

The Ninth Circuit reached a similar conclusion in *Zappos*. In that case, hackers stole PII of Zappos's customers, including names, account numbers, passwords, email addresses, billing and shipping addresses, phone numbers, and credit and debit card information. *Zappos*, 888 F.3d at 1023. Although the stolen information did not include social security numbers, the Ninth Circuit determined that the plaintiffs had adequately alleged an impending risk of identity theft

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

because the hackers could exploit the information taken in the data breach to get even more PII. *Id.* at 1027. The court explained that "Zappos itself effectively acknowledged [this possibility] by urging affected customers to change their passwords on any other account where they may have used 'the same or similar password.'" *Id.*; *see also In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014) (finding that "the risk that Plaintiffs' personal data will be misused by the hackers who breached [the defendant]'s network [was] immediate and very real," when hackers accessed names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates).

The PII stolen from the 2016 Data Breach is far more limited than that in *Krottner* or in *Zappos*. Although the potential repercussions of a hack of one's social security number or credit card information are straightforward—social security numbers may be used for identity theft and credit card information could be used to rack up fraudulent charges[2]—Plaintiff fails to explain *how* gaining access to one's basic contact information and driver's license number creates a credible threat of fraud or identity theft. *See Antman v. Uber Techs., Inc. (Antman I)*, No. 3:15-cv-01175-LB, 2015 WL 6123054, at *10–11 (N.D. Cal. Oct. 19, 2015) (similarly concluding that an allegation that a theft of names and driver's licenses, without more, is insufficient to establish a credible threat of immediate harm).

Plaintiff attempts to sidestep this issue by claiming that identity thieves could use the stolen information to get *other* personal information. *See Opp.* 8:9–14. However, unlike in *Zappos*, where the plaintiffs described the way in which hackers could commandeer their accounts and identities using the information taken from the defendant, here, the Court cannot discern, and Plaintiff does not sufficiently explain, how the hackers could use one's contact information and driver's license number to gain access to additional personal information.

Plaintiff next claims that Defendant's representations concerning the scope of the data compromised in the 2016 Data Breach "cannot be trusted, given Defendant's dishonesty concerning this breach, its actions in paying off the hackers instead of disclosing it, and its admitted disclosure of more types of information in the nearly identical, earlier 2014 Data

[2] Further, as the Ninth Circuit points out, "Congress has treated credit card numbers as sufficiently sensitive to warrant legislation prohibiting merchants from printing such numbers on receipts—specifically to reduce the risk of identity theft." *Zappos*, 888 F.3d at 1027 (citing 15 U.S.C § 1681c(g)).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

Breach." *Opp.* 8:14–19. For one, the Court rejects Plaintiff's attempt to bootstrap negative inferences based on the misconduct already alleged in the complaint. Plaintiff's insistence that the Court draw adverse inferences against Uber based on another data breach in 2014 is also unpersuasive. *See id.* In late 2014, Uber suffered another data breach, but did not disclose it until February 2015, about five months after it first became aware of the incident. *See FAC* ¶¶ 32–34. Uber's initial disclosure stated that the names and driver's license numbers of approximately 50,000 drivers were exposed in the 2014 Data Breach. *Id.* ¶¶ 35–36. In August 2016, Uber notified the victims that, contrary to its earlier representations and notices, additional PII, including "banking information" and social security numbers, were disclosed in the 2014 Data Breach. *Id.* ¶¶ 38–39. Nevertheless, allegations surrounding how Uber may or may not have handled prior data breaches cannot cure Plaintiff's failure to adequately plead a credible risk of immediate harm concerning *this* data breach. *See Antman v. Uber Techs., Inc. (Antman III)*, No. 15-cv-01175-LB, 2018 WL 2151231, at *11 (N.D. Cal. May 10, 2018).

In sum, the Court concludes that Plaintiff's allegations of an increased risk of fraud and identity theft are insufficient to establish a credible risk of immediate harm.

ii. Other Injuries

Plaintiff also alleges that he has suffered other injuries, none of which are sufficient to establish an injury-in-fact. For instance, Plaintiff alleges that he has incurred "time and expenses related to monitoring financial accounts for fraudulent activity." *FAC* ¶ 43. However, mitigation expenses are only relevant if the risk of immediate harm—here, fraud and identity theft—is "real and imminent." *See Krottner*, 628 F.3d at 1143; *Zappos*, 2015 WL 3466943, at *10–11. Because Plaintiff has not pleaded a risk of immediate harm, mitigation expenses cannot establish an injury-in-fact.

Similarly, Plaintiff's contention that he suffered a "loss of value of [his] private information," *FAC* ¶ 43, without any more details, is "too abstract and speculative to support Article III standing." *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1029 (N.D. Cal. 2012); *see also Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301 (N.D. Cal. Dec. 21, 2016) ("In order to show injury in fact under [the theory that the plaintiff's personal information diminished in value, the plaintiff] must establish both the existence of a market for her personal information and an impairment of her ability to participate in that market."). The same is true for his conclusory allegation that the breached caused him a loss of privacy. *See In re*

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

Zappos.com, Inc., 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015) ("Even if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury.").

Lastly, Plaintiff's contention that he has been harmed by the sheer fact that Defendant violated certain state consumer statutes is unavailing, *see Opp.* 8:20–9:2, given that he cannot identify any concrete harm stemming from the 2016 Data Breach in the first place. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016) (holding that a plaintiff cannot "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III").

B. Causation

In support of his opposition brief, Plaintiff has submitted a supplemental declaration, claiming that since the 2016 Data Breach, (1) his 2016 tax return was fraudulently filed by someone other than him, causing him a delay in receiving his tax refund and additional administrative burden when filing future tax returns, and (2) he has had "two credit cards and one debit card" canceled and replaced by issuing banks, because an unauthorized charge was made on them. *See Declaration of Steven Agans*, Dkt. # 63-2 ("*Agans Decl.*"), ¶¶ 4–6. He further states that he is "convinced that the . . . fraud that [he] experienced [was] a consequence of the Uber data breach." *Id.* ¶ 7. However, when addressing a motion facially attacking subject matter jurisdiction, the Court may not consider any information outside of the complaint, judicially noticeable facts, and documents incorporated by reference, without turning the motion into one for summary judgment. *See PNC Equip. Fin., LLC v. Cal. Fairs Fin. Auth.*, No. CV 11-6248 MMM (DTBx), 2012 WL 12506870, at *3 n.23 (C.D. Cal. Feb. 9, 2012). The Court declines to do so here.

Even if the Court were to consider Plaintiff's allegations made in his supplemental declaration, he fails to demonstrate a causal connection between those injuries and the 2016 Data Breach. *See Lujan*, 504 U.S. at 560–61. As explained above, it is not apparent to the Court how the disclosure of Plaintiff's basic contact information and driver's license number could be plausibly used to gain access to his tax return or make fraudulent charges on his credit and debit cards.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	ML 18-2826 PSG (GJSx) CV 18-2970 PSG (GJSx)	Date	August 19, 2019
Title	In re: Uber Technologies, Inc., Data Security Breach Litigation Steven Agans et al. v. Uber Technologies, Inc. et al.		

C. Conclusion

In sum, the Court finds that Plaintiff has not adequately pleaded an injury-in-fact or a causal link between an injury and the 2016 Data Breach. Because Plaintiff lacks standing to pursue his claims, the Court **GRANTS** Defendant's motion to dismiss.

IV. Leave to Amend

Whether to grant leave to amend rests in the sound discretion of the trial court. *See Bonin v. Calderon*, 59 F.3d 815, 845 (9th Cir. 1995). Courts consider whether leave to amend would cause undue delay or prejudice to the opposing party, and whether granting leave to amend would be futile. *See Sisseton-Wahpeton Sioux Tribe v. United States*, 90 F.3d 351, 355 (9th Cir. 1996). Generally, dismissal without leave to amend is improper "unless it is clear that the complaint could not be saved by any amendment." *Jackson v. Carey*, 353 F.3d 750, 758 (9th Cir. 2003).

The Court believes that the defects in Plaintiff's standing are a product of insufficient pleading that may be cured through amendment. As such, the Court **GRANTS** leave to amend. Any amended complaint must be filed no later than **September 19, 2019**.

V. Conclusion

Defendant's motion to dismiss is **GRANTED**. Plaintiff is **GRANTED** leave to amend. Any amended complaint must be filed no later than **September 19, 2019**. Failure to amend by this date will result in the complaint being dismissed *with* prejudice.

IT IS SO ORDERED.